INTERDIGITAL

WHITE PAPER

Spectrum Access System for the 3.5 GHz Band

Submitted in response to Public Notice DA 13-2213
GN Docket No. 12-354

January 2014

InterDigital, Inc. ("InterDigital") hereby submits the white paper entitled "Spectrum Access System for the 3.5 GHz band" in response to the Commission's Public Notice DA 12-2213 (GN Docket No. 12-354).

InterDigital is an industry leader in exploring and developing dynamic spectrum use technologies. Since its founding in 1972, the company has been a wireless pioneer that has designed and developed a wide range of technologies used in digital cellular and wireless products and networks, including 2G, 3G, 4G and IEEE 802-related products and networks. The company actively participates in and contributes to the standards bodies that drive the design and function of each generation of wireless technologies. These bodies include IETF, ETSI, 3GPP, SAE, and IEEE 802 among others.

Some of InterDigital's recent contributions to the worldwide standards have been in areas involving multi-carrier technology, heterogeneous deployments, interference management, dynamic spectrum management, small cell support, relays, machine-type communications, security and video over wireless.

Inter Digital is motivated by its commitment to wireless innovation and believes in the strong potential of spectrum sharing technology to meet unprecedented spectrum demand. InterDigital's Dynamic Spectrum Management (DSM) solutions exploit and aggregate the capacity of underutilized bands to dynamically add more capacity to commercial LTE and Wi-Fi® systems, dramatically supplementing bandwidth. Our Wi-Fi (DSM-Wi-Fi) and LTE (DSM-LTE) solutions are being developed for standards-based interoperability to enable scalable and cost-effective solutions. InterDigital is working actively to lead initiatives within key standards organizations such as ETSI, 3GPP, IETF and 802.11 to foster adoption of spectrum sharing capabilities, and is motivated to work across the ecosystem to drive market adoption of shared spectrum in the 3.5 GHz band.

This paper addresses some of the questions raised in the Commission's Public Notice [1] regarding a minimum set of system requirements and functional parameters for a Spectrum Access System (SAS) operating in the 3.5 GHz band. The paper is structured as follows: the introduction in Section 1 presents a brief background of the SAS and a high level block diagram of the SAS system highlighting the interfaces between the various network entities. Sections 2 to 4 address the focus areas A, B and C outlined by the Commission's call for papers [1], while Section 5 addresses a subset of the topics in focus area D and briefly touches on aspects related to the initial launch.

1 Introduction

It has become obvious that the demand for wireless broadband capacity is growing much faster than the availability of new spectrum and that the future wireless traffic demands also require new wireless network architectures and new approaches to spectrum management. We believe that the development of new technology that enables spectrum to be shared in a dynamic and flexible manner can significantly increase the efficiency of the overall spectrum use.

InterDigital shares the Commission's view that a dynamic spectrum access system building on the TV White Spaces database concept can be used to manage access and to prevent interference between incumbents and other authorized users. We believe that the SAS will be a key component of the 3.5 GHz shared spectrum band, managing the proposed three access tiers. We also believe that the same technology could be utilized in other bands as well.

A high level block diagram of the SAS proposed in [3] is shown in Figure 1. The figure shows that the SAS can interface with users in all three tiers, the Administration and possible other SASs. Regarding the incumbent (Tier 1) users in the 3.5 GHz band, the SAS can interface with both with classified and non-classified spectrum management entities, as shown in Figure 1 below.

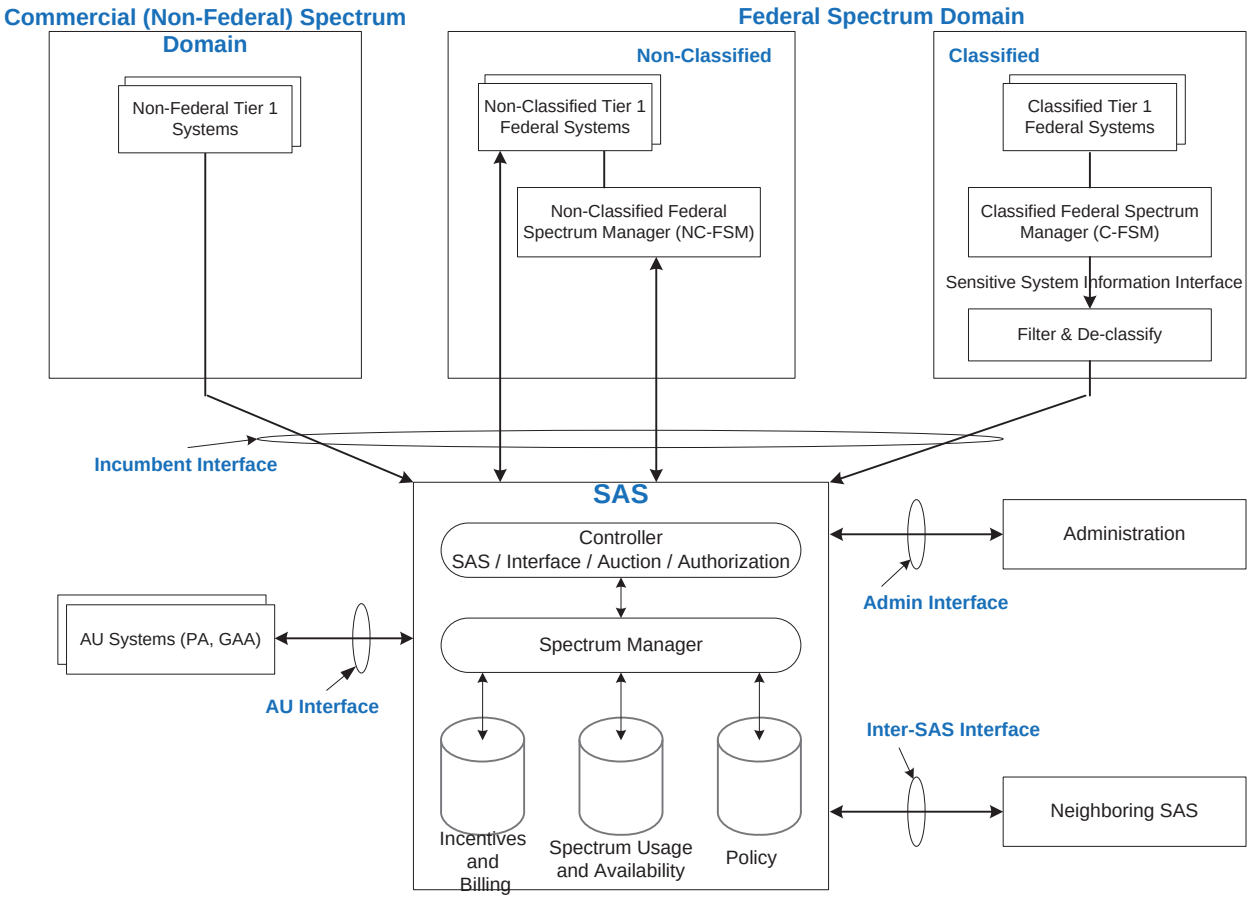

Figure 1. High level diagram of the SAS system Architecture

The SAS can be seen as a sophisticated evolution from the geo-location databases currently being developed and deployed for the operation of White Space Devices in the UHF broadcast band in the US and in other countries. The TVWS geo-location database system implements a simpler 2-Tier system where the main protected incumbent users are terrestrial broadcasting and PMSE. In contrast, the SAS would need to implement a 3-tier hierarchical system that needs to ensure incumbent protection, perform dynamic frequency assignments to Authorized User (AU) systems (Priority Access and GAA users) based on their spectrum requirements and technical characteristics, collect usage metrics from the Priority Access users, as well as (possibly) manage the incentive and bidding system. The information that the SAS database may need to store for effective spectrum management, would include (but is not limited to): geo-location information for incumbent systems (filtered as illustrated in Figure 1 above in case of sensitive federal systems), time, frequency and bandwidths of the systems accessing the spectrum, transmit powers and spectral masks, radio access technologies being used, receiver sensitivity requirements (where needed or applicable for coexistence purposes), and so on. As shown in Figure 1, the SAS would need to interface with the incumbent systems, AU systems, the Administration, and possibly with other SASs. The incumbent systems may be federal users, classified or non-classified, as well as non-federal users. The non-federal incumbent system would interface directly with the SAS, through the "Incumbent interface" described in Section B.1. The federal non-classified incumbent systems may either interface directly with the SAS via the incumbent interface, or if applicable, connect to a Non-Classified Federal Spectrum Manager (NC-FSM) that is further connected to the SAS. The classified federal incumbent users (such as military/Navy radar systems operating in the S-band) would interface with a Classified Federal Spectrum Manager (C-FSM) that would be connected to a filtering entity that applies the appropriate measures to ensure protection of sensitive information. Further details on the Incumbent interface, as well as on the AU interface, Administration interface and the responsibilities of the SAS entities are presented in Sections B.1, B.3 and B.4.

In addition to a regulatory framework that would define certain policies on how the SAS may assign spectrum efficiently to the different tiers, we believe that other keys to the success of the 3-tier spectrum sharing approach are the incorporation of an incentive system (to encourage the incumbents to share their spectrum, when and where it is not fully used), and a dynamic bidding mechanism (that would encourage the Priority Access and GAA systems to efficiently use the spectrum). As a result, the protocols implemented in the SAS would need to address the aspects of supply, demand, as well as incentive and pricing.

2 Focus Area A: General Responsibilities and Composition of SAS

A.1. Scope of the SAS's responsibilities

We agree with the Commission that the effectiveness of the proposed dynamic spectrum sharing regime depends on proper spectrum authorization and management among the various users that would operate in the 3.5 GHz Band. The proposed SAS is essential to realizing this goal, especially because the

emerging technologies will be able to cover both authorization and spectrum management related tasks.

In our view the SAS can enable the use of the 3.5 GHz band by assigning spectrum individually to the authorized access users, following the principles defined by a policy (made available by the Commission). The assignments may be done in a manner that optimizes the overall use of the band. Metrics that reflect the spectrum usage effectiveness (as discussed for example in [4] and [5]) may be used for the objective function, and a set of constraints may be defined, to enable PA network nodes to provide a required QoS for their end users.

There may also be reasons to do reassignments when the radio environment or the spectrum requirements of the users change. The SAS may collect information about the spectrum usage, its trends and patterns over the time and about possible interference levels in various places. This information may be used for reporting, for optimizing the spectrum assignments and for interference mitigation.

De-conflicting the use of the band is possible by making the individual assignments in a manner that takes into account the deployments of the systems and their protection criteria. This allows avoidance of harmful interference. Information about interference measured by the users can allow the SAS to avoid assignments that would suffer from emerging interference, to identify the source of interference and instruct the respective systems to modify their operational parameters so that creation of harmful interference is avoided or minimized, or to terminate the assignments of interfering systems.

SAS's responsibilities to enable and de-conflict the access to spectrum manifest in the spectrum assignments (as well as reassignments when the channel conditions change or the incumbents need to reclaim the spectrum) and protection of the incumbents and the PA users from harmful interference, and through the joint use of signaling to the access users to vacate the spectrum, and of a "time-to-live" (TTL) mechanism (as defined in the PCAST report [4]). An aspect of de-conflicting the spectrum use is the SAS's responsibility to provide the requested quality of access (QoA) for the PA users, which in turn allows them to provide the required QoS. When a PA user experiences sudden performance degradation so the QoS decreases below the requested threshold, it may perform additional measurements to identify the cause of the degradation. If the PA user determines that the degradation is due to external interference, it may report it to the SAS. This event and the associated signaling to the SAS will be referred to as "QoA event" in the remainder of this paper. Once the SAS receives a QoA event report from a PA user, it needs to verify the validity, and based on this, the SAS may take mitigation measures. One example may be restricting the access of GAA users located in the vicinity of the affected PA user.

When the SAS assigns spectrum to Priority Access and/or GAA users, it would also assign a validity time (or "time-to-live (TTL)") for which the spectrum assignment is valid. The use of a Priority Access License (PAL) with a 1-year granularity as proposed by the Commission in [2] is a good way to implement the validity time for the Priority Access (i.e. Tier 2) users. Such duration and the possibility to aggregate consecutive one-year terms can allow the PA users the regulatory certainty they need for justifying their network investments. At the same time, a more granular validity time may be appropriate for the GAA users, e.g. in the range of days, or weeks up to months, depending on the application. This would

effectively result in "longer TTL" for the PA users (1 or several years, up to a maximum cap still TBD), and shorter TTL for GAA users. Upon the expiration of the TTL, signaling may be used to renew the GAA assignments. The granularity of the TTL for GAA users, as well as the mechanism to signal the TTL renewal (or denial) should be carefully specified, taking into account the nature of the deployed services, in order to minimize the signaling overhead.

To summarize, in our view the SAS can take care of both authorizing the users (if so required, based on the principles of the policy defined by the Commission), and managing the use of the band. It can define the operational parameters and spectrum assignments for the users in a dynamic radio environment while optimizing the overall spectrum use in the band and protecting the required users from harmful interference. It can also take care of the economic framework in accordance with the policy defined by the Commission. The economic framework may cover economic incentives for the incumbent, various types of spectrum auctions, including periodic and on-demand auctions, collection of fees etc.

A.2. Key elements of the SAS

Key System elements of the SAS

The foreseen key system elements of the SAS are the SAS controller, a spectrum manager, and databases, as shown in Figure 2.

The SAS controller (SAS / interface / authorization / auction):

- The **controller** is responsible for controlling the interfaces between the SAS and the other network entities illustrated in Figure 1, specifically: the Incumbents (Tier 1) interface, the Authorized User (AU) interface, inter-SAS interface (if applicable, in case of a distributed multi-SAS architecture), and interfacing with the Administration (the Commission) through the "Administrative" interface, to upload the applicable policies and for authorizing the access users. If an incentive and auction system is supported, the SAS controller could be the entity within the SAS responsible for controlling the auction process, the bids and asks for the PALs.

The **spectrum manager**:

- The **spectrum manager** is responsible for performing spectrum assignments and reassignments, together with their optimization, to make efficient use of spectrum, while ensuring both the incumbent protection and quality of access, i.e. sufficient amount of spectrum and protection from harmful interference for PA users. It can also collect and analyze measurement results collected from users, including the QoA events.

SAS **Databases**:

- The **spectrum usage and availability database**: this is a database in which the current spectrum usage and availability can be obtained and can be dynamically updated by the SAS when new spectrum assignments are made, spectrum usage changes, etc. The database will maintain the current spectrum that the SAS has available to assign to PA or GAA users, based on what the Incumbents have indicated is available and currently unused by the Incumbents. In addition, the

database will maintain the spectrum that has been assigned to a PA or GAA system, as well as additional usage parameters associated with that spectrum usage (e.g. the maximum transmit power used by a PA or GAA system or associated transmission range, the time of use, etc.). The database would also store the technical information provided by each user upon registration, including where applicable the protection criteria. The spectrum usage and availability database may also store selected measurements from the network nodes (e.g. interference metrics, radio maps), which can be used to support the spectrum assignment algorithms.

- The **policy database**: this database may be used for storing the policies from the Administration (such as the overall approach for authorizations and assignments for PA and GAA users), information on issued individual authorizations, information on the spectrum usage in adjacent bands and/or geographical areas (including transmit characteristics and protection criteria). This approach allows amendments of the policies to be reflected into the operation of the SAS in real time.

- The **incentive and billing database**: If an economic framework that can enable incentives for the incumbents, and auctions for the PALs is considered, then the SAS may need to dynamically track the amounts that each PA system must pay for its spectrum usage (billing), and the amounts owed to each incumbent system whose spectrum has been assigned for use to another system by the SAS (incentive). This can be achieved by using the incentive and billing database within the SAS.

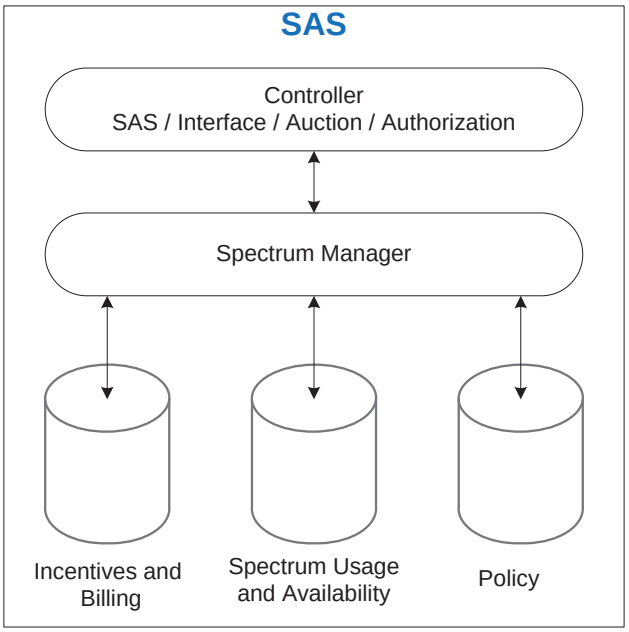

Figure 2 Elements of the SAS

Responsibilities

In our view the preferred solution would be to allow commercial entities to develop and operate multiple SASs, as this would encourage increased competition, foster innovation, and potentially lower the costs of development and deployment of the SAS, as well as the cost of using the services of the SAS as there would be a possibility to cover at least some of the costs through collection of fees or by portions of the auction prices.

Commission role and oversight

Some Administration (i.e. Commission) involvement with the SASs would be needed, as there would be a role for the Commission related to the definition of relevant policies, authorizations and supervision. The Commission would have to specify the high level requirements for the SAS; before the approval for starting the operation of the system, the Commission will ensure that the operation of the SAS fulfills the policy and implements the required protection of the Incumbents and the PA users.

It should be noted, that employment of an entity such as the SAS and the communication between the SAS and the Administration can facilitate new spectrum use authorization approaches and flexible admission control, which can both significantly contribute to the proposed advanced spectrum management approach. In the following we describe some of the possible elements for the Administration involvement.

The communication with the Administration could consist of an automated entity managed by the Administration, such as a database, active entity, human interface, secure web-site, etc. Depending on the implementation, the automated entity might need to be complemented by human actions.

The Administration could provide the SAS with essential operational information already before the actual spectrum requests and assignments can take place. This would allow the Administration to authorize the SAS, to communicate the relevant policies and possible information about the issued authorizations of the involved players. Depending on the policy of the Administration, the SAS might be authorized to issue individual authorizations on behalf of the Administration to the Users that request access to spectrum, and in that case the SAS needs the authorization criteria from the Administration. There may also be a need for the SAS to get information about the spectrum use within its geographical coverage area in bands adjacent to the bands that it manages and on the co-channel spectrum use adjacent to its geographical coverage. The Administration can provide SAS with such information, which it would store to its databases. The dialogue may be repeated periodically or on a need basis, if e.g. the policy or the use in the adjacent frequencies changes, in line with the policy issued by the Administration. The communication between the SAS and the Administration may also include the SAS reporting to the Administration about the spectrum management activities that took place, spectrum usage and interference incidents that have taken place.

The policy obtained by the SAS from the Administration may also contain a list of PA users or GAA users that are authorized to use the services of the SAS. For instance, a network operator may request the

authorization from the Administration to use shared spectrum in a particular operational area. If the operator fulfills the required criteria, the Administration allows that operator to have access to shared spectrum as requested, in a specific band, geographical region, and time. This authorization is then indicated by the network operator to the SAS when the operator registers with the SAS. When that specific operator makes a request for spectrum from the SAS, the SAS may then assign spectrum to the operator based on the information obtained both from the operator, and from the Administration.

The policy may also be used by the SAS to prioritize the different PA users or GAA users in terms of spectrum to be assigned to each, or to define a maximum amount per PA user or GAA user in the situations where there is a scarcity of spectrum.

Authorizations

The Commission proposes in [2] to use one year non-renewable PAL's which would allow the PA's to use of certain amount of spectrum in a certain location and over a certain period of time. In a way such PALs could be considered as licenses (individual authorizations) that at the same time define the duration of the spectrum assignments, i.e. one year. That approach is indeed feasible and practical, and it can be used for the initial system deployment. However, the use of the SAS may facilitate use of individual authorizations that have durations independent of the durations of the assignment, whereas the durations of the assignments may be handled separately, according to the needs of the users. The use of the SAS can offer new possibilities for issuing the authorizations, as shown below.

- All Users that have been individually authorized (AU's) by the Administration are allowed to register with the SAS and are entitled to spectrum assignments. A mechanism like use of Authorization key or Certificate may be employed for the AU's to indicate to the SAS in a reliable manner that they have the required authorization. In practice the authorization may allow the PA user to attend the next auctions and success in the auction will result in the requested spectrum assignment.

- The SAS may be allowed within the policy to contact the Administration on behalf of the users, and get the authorizations based on delivering the required information, which may include the identity, spectrum requirements and technical characteristics of the users. Like for most communication between different entities and the SAS, for all these steps secure communication is needed. The Administration would issue the individual authorizations, which include the validity time of the authorizations and possible operational conditions.

- The SAS may be authorized by the Administration to authorize the users. This may be done based on pre-defined criteria in line with a policy from the Administration.

- In case there is no need for individual authorizations the SAS may allow any user to register and get assignments, or the SAS may choose the users that will get registered based on the policy issued by the Administration or on some other criteria. This may apply especially to the GAA users, which may be licensed by rule.

The individual authorizations would need to be renewed when the current authorization expires, or if there are technical, operational or commercial changes that are specified in the policy. The same methods as used originally can be employed the authorization renewal.

A.3. Impact of rules on the system architecture

A key rule that impacts the system architecture is whether the SAS is commercially operated (as illustrated in Figure 1), or operated by the Administration. In the first case, the Administrative interface needs to be specified between the SAS and the Administration (including the information elements, protocol and signaling), procedures for security and authentication of the SAS. Additionally, a set of rules needs to be defined to clearly specify the responsibilities of the SAS for authorization, assignments / reassignments and so on. In the second case, the Administration functionality may be incorporated in the SAS, resulting in different signaling requirements for the administrative interface.

For each alternative (commercially operated or Administration operated SAS), the next key decision is whether a single SAS or multiple SAS system is desired (in other words, a centralized vs. a distributed architecture). Clearly a distributed system employing multiple SASs would require the definition of an Inter-SAS interface, with its associated synchronization procedures and signaling. Although this may result in additional signaling overhead as compared to a centralized single SAS system, we believe that a multiple SAS system with commercially operated SASs has the potential to encourage competition, with positive benefits to innovation and costs (as indicated in Section A.2). Operation of multiple SASs in parallel may also increase the reliability of the whole arrangement by allowing improved availability and redundancy.

Lastly, if the regulatory environment allows or requires the use of economic incentives for the incumbents and auctions for the PA users for awarding the available PALs, the system architecture would need to support both the technical framework (spectrum assignments / reassignments, incumbent protection, etc.) and the economic framework (such as signaling to support automated auctions).

A.4. Considerations on interoperability

To ensure interoperability between multiple SASs provided by multiple vendors, and between SASs and AUs, the interfaces illustrated in Figure 1 need to be standardized, as follows: the AU Interface (PA/GAA to SAS), Incumbent interface (incumbent users to SAS), Inter-SAS interface, and the Administrative interface (SAS to Administration). Additionally, to be authorized to operate as SAS, the equipment provided by the various vendors must prove compliance with Incumbent protection criteria and the possible channel evacuation requirements. Once the information that needs to be exchanged between the various network entities is identified, the interface protocol(s) may be developed by building upon the existing PAWS protocol [6].

It is expected that the spectrum optimization and assignment algorithms, as well as the pricing algorithms can be vendor specific, which allows room for technical innovation and differentiation between the SASs in the market place.

A.5. Interaction between the SAS and the incumbent systems

The SAS would interact with each Incumbent using secure communication over a standardized interface. The interaction would cover exchange of both technical and economic information, if the economic incentives are in use.

Initially each Incumbent would have to register with the SAS. Secondly, the Incumbents would indicate what frequencies are made available, and the associated technical, operational and economic conditions. The SAS would make some of or all offered spectrum available for other users, and take care of actions related to the economic incentives towards the Incumbents.

The Incumbents may also have a right to claim back the spectrum made available on certain agreed conditions, and the SAS would have to have the required capabilities to implement the possible reclaim.

We believe that also classified Federal spectrum can be made available for the PA and GAA use through the use of the classified Federal spectrum manager, which will need to communicate with the SAS in a secure way, by filtering information about classified spectrum usage. This can be achieved through sending a limited amount of information only about the available spectrum, i.e. by performing a subtask of the overall work otherwise done by the SAS (which would require handling of sensitive information about the spectrum usage and physical characteristics of the classified spectrum). Some properties of the filtered spectrum information could include: the absence of any PHY layer characteristics of the incumbent systems with which sharing will be done (e.g. modulation scheme, spectral masks, etc.), the absence of detailed geo-location information (such as location of stations, range, etc.), as well as the ability to conceal exact time, location and frequency of spectrum usage in a band by not making all available spectrum usable by the SAS. Additionally, the classified Federal spectrum manager could have additional flexibility to refuse certain spectrum usage based on the identity of the PA / GAA user proposed for usage, as well as the ability to modify or set certain spectrum usage parameters initially proposed by the SAS.

3 Focus Area B: Key SAS Functional Requirements

B.1. Minimum information exchange within an SAS system

The functionality of the SAS (in terms of regulatory policies and spectrum assignments), as well as the functionality that each interface illustrated in Figure 1 need to support are key factors that determine

the minimum control information that must be exchanged between the various entities of the SAS system.

As shown in Figure 1, the **Incumbent interface** can be used to connect to a classified federal spectrum manager (C-FSM) in order to make use of available spectrum under classified federal control (e.g. military spectrum usage). In this case, it is assumed that the C-FSM entity may apply specific filtering and de-classification techniques to protect sensitive information from being signaled to the SAS. The Incumbent interface can also be used to interface to a non-classified federal spectrum manager (NC-FSM) in order to make use of federal spectrum that is not under classified federal control and potentially, directly with non-federal (or commercial) Incumbent systems.

To enable efficient incumbent protection and spectrum sharing by the Incumbent users, the following information needs to be exchanged on the **Incumbent interface**:

- Spectrum availability information from the Incumbent system. This includes the location, frequency and duration for which the spectrum is made available for sharing. The spectrum availability information may be mapped by the SAS to blocks of PALs using the geographical dimension of the PALs, as indicated in paragraphs 14-16 of [2].
- Incumbent protection criteria
- Channel evacuation criteria, in case the Incumbent may need to reclaim part of or all spectrum back for its use.
- Lastly, if the auction mechanisms are to be employed, auction related information (e.g. minimum price, bids and asks) to be exchanged between the incumbent systems and the SAS.

Once the information elements (IE) exchanged on this interface are defined, it may be beneficial to evaluate the feasibility (and benefits) of extending existing protocols, such as the PAWS protocol [6] to support this interface. The control messages to be signaled on the Incumbent interface could include:

- Network registration request / response
- Network reconfiguration request / response
- Spectrum availability indication / acknowledge
- Spectrum release indication
- Spectrum reclaim request

The **AU interface** can be used connect the SAS to PA and/or GAA users. As the Incumbent protection is essential to the system, it will be taken into account by the SAS in making the assignments. The possible channel evacuation requirements must be signaled by the SAS to the PA / GAA users. Moreover, in order for the SAS to enable the provision of QoS for the PA users, the SAS would need to collect spectrum requirements and protection criteria from the PA users. In addition, the SAS can collect spectrum usage metrics from the infrastructure nodes (e.g. RAN O&M, (e)NB/BS, AP). These could be used by the SAS to prepare for coming spectrum requests and help to determine whether to accept or deny TTL renewal requests (if the concept of TTL is used for the GAA users), and to determine the new channel assignments.

Additionally, when an Incumbent user needs access to the spectrum immediately, for example in an emergency situation involving a mission-critical incumbent system, it would signal the request to the SAS, which would then signal the spectrum evacuation commands to the affected PA and GAA users to vacate the spectrum.

In summary, the information that needs to be exchanged through the **AU interface** between the SAS and the PA/GAA includes:

- Method of access (as PA or GAA), spectrum request (location, bandwidth and availability time).
- Protection criteria for the PA systems.
- AU device capabilities and network information (e.g. RAT, transmit and receive characteristics, usable frequency range, sensing capabilities, coverage or deployment characteristics, antenna height).
- Allowed operating conditions for the AU's (e.g. available spectrum, transmit power or maximum transmit power to be used by the AU).
- Channel evacuation requirements (for cases when incumbent users need to reclaim the spectrum).
- Pricing / auction information (bids and asks) if the system supports automated auctions for PALs.
- Measurement reports sent by the infrastructure nodes eNBs, APs to the SAS, in support of the spectrum assignment algorithms run by the SAS.

The control messages to be signaled on the **AU interface** include:

- Network registration request / response
- Spectrum request
- Spectrum assignment response
- Spectrum use indication
- Spectrum evacuation command /confirm
- TTL renewal indication (may be used for GAA users)
- Measurement reports
- QoA Event (as defined in Section A.1).

The **"Administrative" interface** (between the SAS and the Administration) is used to upload the applicable policies to the SAS, to communicate information on issued individual authorizations, information on the spectrum usage in adjacent bands and/or geographical areas (including transmit characteristics and protection criteria).

B.2. Parameters configured by the SAS

The spectrum manager entity of the SAS calculates the frequency assignments in response to a spectrum request from PA/GAA users based on their technical characteristics and network deployment information and determines the operational parameters of the PA/GAA that ensure incumbent

protection. The SAS signals these parameters to the PA/GAA users at the time of the spectrum assignment. The information includes:

- Frequency assignment (frequency bands (channels) to be used, availability duration (e.g. PAL duration or TTL) and locations or area).
- Allowed maximum transmit power for both the network nodes and the mobile terminals of the PA/GAA system. This assumes that the technical characteristics of the nodes (such as device category/class or individual technical characteristics) and the network deployment characteristics were previously signaled to the SAS (possibly during the registration) and that those were taken into account in the frequency assignment algorithms.
- Channel evacuation requirements (if required)
- Sensing configuration (if measurements/sensing in use)

Optionally, the SAS may signal to the PA user requests for spectrum re-assignment or evacuation, or limited information related to the spectrum usage by the nearest neighboring systems, to be used in connection with possible measurements (sensing). This information may include: the location of the network node, channel(s) of operation, RAT type.

B.3. Network entities interacting with the SAS

We agree with the FCC assumption that infrastructure nodes, like Radio Access Networks Operation and Maintenance (RAN/O&M), Node B/Base Stations (eNB/BS), or Access Points (APs) would interact with the SAS and provide SAS with spectrum offers/requests, and provide the User Equipment/Mobile Stations/Access Terminals (UE/MS/AT's) with relevant operational parameters and updates.

B.4. Capabilities of the network nodes reported to the SAS

For efficient frequency assignments, and to reduce the interference between adjacent systems, the Spectrum Manager entity within the SAS needs knowledge of the location of the network nodes of each cell, tuning range, transmit power range and adjustment step size, as well as RAT specific device class (which defines the receiver characteristics and interference mitigation capability). Other information may include: sensing capabilities, channel switch time, and so on. The capabilities listed above need to be reported by the network nodes to the SAS, either upon registration, or upon spectrum requests. This is similar to the reporting specified in the PAWS protocol [6], by the master device to the TVWS database. Thus the PAWS protocol may be a good baseline that can be extended to support the interface between the AU network nodes and the SAS. It should be noted that reporting the capabilities such as those listed above should be done in such a way to minimize the signaling overhead. This may be achieved by reporting the device class or category, as specified in the standards (e.g. 3GPP or 802.11) instead of reporting the capabilities individually, and by doing this only in connection with the

registration or when changes occur. Additional mechanisms to abstract the information can be devised as needed.

B.5. Update mechanisms

The need for assignment updates by the SAS occurs e.g. when spectrum is made available for sharing by the Incumbent users, and when the incumbent users reclaim the spectrum. Additionally, frequency requests leading to assignments and reassignments to PA/GAA users also lead to assignment updates. Changes in policy from the Administration can also trigger assignment updates. And finally, if the duration of the PAL's is in the order of a year, there may be technical changes in the deployed networks and changed protection criteria, which could also result in assignment updates.

Periodic or event triggered signalling can be used for the assignment updates. It should be noted that the need to update some assignments may lead to optimization (i.e. repacking) of all assignments, depending on the nature and timing characteristics of the spectrum use by the AU's. Such approach may help in keeping the overall use of the band optimized, thus maximising the efficiency of the overall spectrum use.

As the updates need to be conveyed to the network entities (SAS, incumbent users, AU infrastructure nodes, and the Administration), the update information needs to be defined for all system interfaces, as shown below.

Incumbent interface:

- Updates are needed when incumbents have available spectrum that can be shared (so they need to signal the spectrum availability to the SAS), and when the incumbents need to reclaim the spectrum. In both cases, the signalling is event triggered. The frequency of occurrence of these events depends on the type of incumbent. The message structure and content should be designed in such a way to minimize the overhead, to make it possible to support a more dynamic system.

AU interface:

- SAS to AU network nodes: updates are needed when the SAS makes a spectrum assignment or reassignment, which needs to be signaled to the appropriate AU node. The frequency assignments/reassignments may occur periodically (associated to auctioning of the PALs), or be triggered by either spectrum requests from PA users, or spectrum reclaim requests by incumbent users. As a result of a spectrum reclaim request by an incumbent user to the SAS, the SAS spectrum manager may run a frequency reassignment, and/or it may need to send a spectrum evacuation message to the appropriate AU.
- AU network nodes to the SAS: updates are needed when AU users send spectrum requests to the SAS. Additionally, while a PA user system operates in the shared spectrum, it may

experience harmful interference that degrades the system performance below a required level. In this case (as mentioned in Sections A.1 and B.1), if the PA user determines that the degradation is due to an external interferer, it detects a "quality of access" event (QoA event), and it may report it to the SAS, for a possible frequency reassignment or other measures.

Administrative interface:

- If the Administration updates any of the relevant policies covering the operation in the shared spectrum, the SAS need to be notified accordingly, in order to update their policy databases.

Inter-SAS interface (for multi-SAS systems):

- In addition to the events mentioned above (spectrum availability / spectrum reclaim requests by incumbents, spectrum requests by AUs, spectrum assignments and reassignments to AUs and QoA events reported by PA users), additional information may need to be signaled between SASs. For example, in the early stages of the system deployment, different SAS providers may be certified and receive authorization to operate, at different times. As a new SAS comes on-line, provisions need to be put in place for the existing SASs to be notified of the new SAS, such that the system remains in synch.

Given the nature of the spectrum being shared, as well as the nature of the PA users using PALs, and the GAA users, we expect that the signaling associated to the system updates is a combination of periodic signaling and event triggered signaling. The periodicity may be applicable to the PA users, and it may be tied to the time duration of the PALs. The frequency of occurrence of the event driven signaling depends on the type of the incumbent (how frequently the spectrum becomes available for sharing, and how frequently it may be reclaimed back); it may also depend on the PA users reporting of the QoA events.

Lastly, it should be noted that the traffic resulted from system updates may be different across the interfaces listed above. Specifically, less traffic is expected on the Incumbent interface as compared to the AU interface.

B.6. Security and privacy

Security is very important for the operation of a spectrum management system based on the use of SAS. Communication with the SAS contains potentially confidential information, and thus only authorized recipients should be able to receive the information and communicate securely with the SAS. Secure communication should be used over all the interfaces (Incumbent, AU, Administrative and Inter-SAS interface), to ensure confidentiality and integrity protection.

A strong authentication procedure is also a key system requirement, to ensure only authorized parties have access to the SAS services.

B.7. Synchronization of multiple SASs

The experience of TVWS (where multiple database providers are certified by the FCC and they can each provide different add-on services) suggests that a scenario with multiple SAS could be commercially possible. In particular, the presence of multiple SAS with overlapping geographical coverage may allow competition based on the services or efficiency of the spectrum assignment algorithm, thus driving the overall price of spectrum down (if auctions are in use), or providing the incumbents with different incentive options for their spectrum.

If multiple SASs are employed, then inter-SAS technical measures, such as synchronization arises, to ensure efficient spectrum assignments, while managing the interference between adjacent systems are required.

The specific synchronization needs depend on how the system is configured, with respect to the coverage area, the frequencies to be managed and the incumbent and AU managed by each SAS. In the likely scenario where overlap occurs between SASs, the "Spectrum Usage and Availability" database illustrated in Figure 2 need to be synchronized, in order to prevent conflicting spectrum assignments from being made by different SASs. This means that once a SAS makes a frequency assignment/reassignment to AUs, or when spectrum is either made available or reclaimed by an incumbent, the relevant information needs to be shared between all SASs. This information includes:

- incumbent protection and deployment info
- PA and GAA assignments (including the RAT used by the PA/GAA)
- PA protection info

Additionally, as mentioned in Section B.5, synchronization of the databases is needed once a new SAS is brought on-line.

It is important, that the control traffic created by the inter-SAS synchronization is minimized. As an example of minimizing the control signalling, the deployment information may be abstracted by using some form of PAL identification (there would be a 1-to-1 mapping between the PAL ID and the frequency and location, using the location units agreed upon in the proceeding). Also, the PA protection criteria may be abstracted by using standards defined QoS (possibly expanded to include max interference limits).

It may also be beneficial to reduce the overlap of responsibilities of the different SASs, in order to reduce the need for constant exchange of synchronization info. This could be done e.g. by reserving an own sub-band for the SASs to manage, even if the incumbents and the geographical coverage areas would fully overlap.

4 Focus Area C: SAS Monitoring and Management of Spectrum Use

C.1. SAS mechanisms for monitoring of spectrum use

The SAS can monitor the spectrum use through reception of traffic and measurement reports from the AU's, and by analyzing them.

The reporting may comprise of traffic information and usage of the channels by the AU's. The SAS may detect traffic patterns from the reports, which can help in ensuring the timely availability of sufficient spectrum for the PA users, even if their spectrum requirements would be time dependent.

The measurement results can also be utilized by the SAS in optimising the spectrum assignments to correspond with the specific protection criteria of particular AU's. The SAS may also act in case interference is detected, either by avoiding completely the usage of the channels where significant interference occurs, by assigning the "cleanest" channels to users that tolerate least interference or if possible by reacting on the source of interference. This would require that the SAS can identify the source of the interference and that its operation is under the control of the SAS.

Detection of spectrum use

Monitoring the spectrum use may be performed by the SAS to ensure incumbent protection, efficient use of the spectrum, and optimize spectrum assignments/re-assignments. To enable spectrum monitoring by the SAS, the AU's network nodes need to send measurement reports to the SAS. The network node of each AU (that has an active spectrum assignment) may collect measurements from the mobile terminals (MT) connected to it; the network node (BS, eNB, AP) needs to aggregate the MT measurements into a single metric. Measurements may also be performed by the network node. Both these measurements (performed by the network node and the aggregated results) need to be reported periodically to the spectrum manager within the SAS.

It may be desirable for the SAS to have the ability to configure the periodicity of the measurement reports from the AUs, such that the signaling overhead does not become too large, while still providing relevant and timely metrics information to be used by the spectrum manager function.

Possible metrics that can be reported by the AUs include: the average noise level, average interference, per channel RSSI, submitted traffic load, and so on.

As the metrics listed above are used by the spectrum management entity for channel assignments / re-assignments and interference mitigation purposes, they may also be leveraged to determine if the spectrum is used at a certain location/frequency/time. For example, the average over-the-air data rate (or the average throughput), normalized to the assigned BW, and compared to a threshold, may be a criterion to detect the spectrum use. As it is conceivable that both Wi-Fi and LTE may be used as technologies for the small cells in the 3.5 GHz band, the metric may further be normalized by the peak data rate for that technology (possibly for a baseline configuration of 1 Rx / 1 Tx), then compared to a threshold in the range of 0 to 1. Using the over-the-air data rate may not provide an accurate indication of the spectrum use, however. This is because the submitted load may be small and bursty, which may correspond to a low utilization of the channel. The effective throughput may be used instead (provided that it is normalized to real time, instead of sub-frame (for LTE) or packet duration (for Wi-Fi).

Detection of spectrum misuse

Incumbent protection is one of the key elements for the success of spectrum sharing in the 3.5 GHz band. As such, the SAS should be able to detect scenarios of spectrum misuse that may lead to the generation of harmful interference to the incumbent systems. Examples of such scenarios include: AU not evacuating the channel upon evacuation commands from the SAS, AU transmitting in a channel not assigned to it or at a higher power than the maximum allowed Tx power, and thus creating either adjacent, or co-channel interference to an incumbent or to another AU.

Another example of spectrum misuse is a GAA user transmitting at a higher power than assigned, in the vicinity of a PA user, resulting in inter-AU interference and the degradation of the QoS experienced by the PA user. This scenario will be further discussed in Section C.2.

Dedicated sensing nodes for detection of spectrum use/misuse

Another possible approach to detecting the spectrum use (or misuse) could be to deploy dedicated sensing nodes across the network. The sensing nodes may be operated either by the SAS operator, or the Administration, and they would be configured to periodically report spectrum measurements (such as averaged and/or aggregated PSD across the band of interest). The advantage of this approach as compared to relying solely on measurement reports from the AU network nodes, is that it does provide an independent (3rd party) observation of the spectrum use. For this approach to be viable, the sensing nodes should be low cost; additionally, a trade-off analysis is needed to determine the amount of data that needs to be signaled to the SAS, as well as the reporting frequency. The SAS could then use the reported sensing results, in conjunction with the "spectrum usage and availability" database, to detect if the spectrum is used at a certain location, or if unauthorized access is detected.

C.2. Inter-AU interference detection and reporting

Once a PA user is assigned a channel for a given time to operate above a specific required quality, it can monitor continuously the quality of its operation on the assigned, active channels. The PA user may also monitor in the background other channels than those it is actively using. For Wi-Fi systems, examples of monitored performance metrics can be the transmit rate, medium access delay, frame error rate, RSSI and so on.

As indicated in Section C.1, the AU (both PA and GAA) may transmit periodic measurement reports to the SAS (for the active channels being monitored). If another AU (PA or GAA) starts using the channel in the proximity of the original PA user's geo-location, so that the user detects a degradation of its quality of operation, the original PA user may trigger extended measurements to determine the cause of performance degradation.

The extended measurements would be performed by the AU network node to evaluate if the cause of degradation is internal (e.g. congestion, or low SNR due to operation at cell edge), or if an external

interferer is present. If as a result of the extended measurements, the AU network node determines that the cause of performance degradation is an external interferer, the node may signal a “QoA event” to the SAS to report the interference.

When the SAS receives a “QoA Event” message from a PA user, it is responsible for resolving the QoA issue. The QoA resolution procedure at the SAS can be comprised of three possible actions: validation (confirm that the report is valid), reassignment, evacuation, and reimbursement. The high level procedure is shown in the figure below whereby interference from a user B triggers user A to send a QoA Event message to the SAS which in turn triggers a resolution procedure.

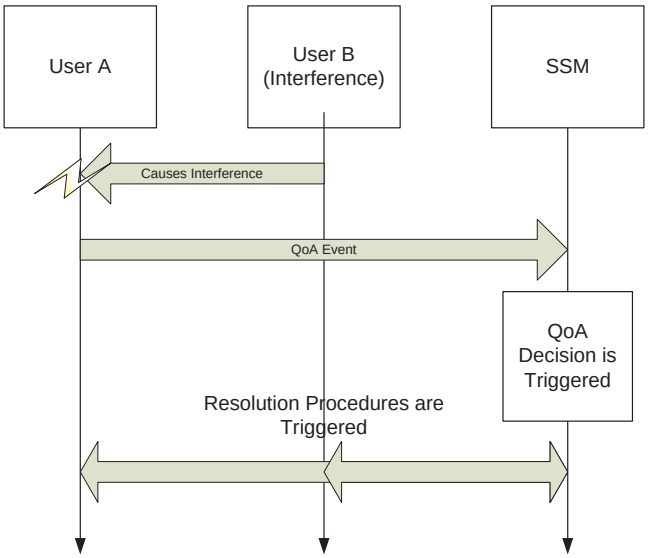

Figure 3 QoA Event detection, reporting and resolution

C.3. Enforcement mechanisms

The risk that devices or network nodes operate outside of the operating parameters authorized by the SAS exists. Such situations may be severe, as interfering devices or network nodes may be extremely difficult to identify and cause harm to the operation of not only SAS services but also the incumbent and AU services. The potential also exists for end-user modification of devices and network nodes in ways that could cause significant harmful interference to critical communications services.

Possibility for remote attestation to the trust state of devices and network nodes may be required in order to protect networks. Additionally, shut down of a device or network node initiated by the SAS may be required. An appropriate legal framework would be needed behind such a drastic measure (e.g., forced shut down of a device will make it impossible to make an emergency call, etc.). From a technical point of view, the event (e.g. device misbehavior) detection would have to be communicated to the SAS for making a decision based on the pre-defined policy and the received event report. The SAS can react by reassigning the user that has suffered from harmful interference, by quarantining the device or

network node or by remediating the interfering device or network node. If a device or network node systematically fails to operate in accordance with the operational parameters defined by the SAS, they may be blacklisted.

It is important to understand that all elements of this interference reporting chain have to be trusted (i.e., the endpoints consisting of the device and the network element, as well as the communication channel).

When a device is trusted and protected against tampering, it becomes possible to store and execute downloaded policies in a protected manner on the device or network node. Such a secure platform architecture provides an additional benefit of relaxing availability requirements for the network policy control. The devices and the network nodes can be made to support both, tamper evidence and tamper resistance, capabilities.

In recent years, trusted computing technologies, which provide assurances and quantifiable evidence of the functionality of a device similar to a hardware implementation or “hard-wired” device, have been developed for practical application to consumer products. These technologies exist in all laptops today in the form of TPM chips and in a rudimentary form in many cellular radios as proprietary security mechanisms. Indeed the Global Platform has specified architecture requirements for secure environments and an applications programming interface for such elements and is promoting the use of secure environments for mobile platforms. Additionally, the Trusted Computing Group is working on creating trust security solutions for mobile platforms, which leverage secure environments as well as a hardware anchored root of trust to ensure trustworthy platform bring up and configuration of the platform and secure environment. Many silicon manufacturers are adopting such requirements to standardize and promote adoption of such technologies in mobile devices to ensure that software may be run in a secure, tamper proof manner.

InterDigital has been developing technologies which leverage the use of trusted computing technologies in the form of secure environments and a root of trust to deliver an overall tightly controlled system level trust security solution. The work has been on the creation of a practical approach to trust security for mobile systems and in particular efficient remote attestation, which separates access control decisions from remediation in the network by balancing trust processing between the mobile platform and the network ([7], [8]).

Such an approach would:

1. Certify the devices for their security architecture and use of trusted computing technologies such as secure elements anchored through a hardware enforced root of trust.
2. Provide for the remote attestation to the trust state of a device, which essentially enables the software based functionality to be “hard-wired”.
3. Enable the remote provisioning, management and update of SAS policies, which may be executed locally on a device.
4. Use the trusted computing base of the device to prevent execution of radio functionality outside of the authorized and provisioned policies.

InterDigital's view is that by promoting the adoption of these technologies, configurable but protected usage policies, may be executed on the devices to enable the safe and legally authorized use of the 3.5 GHz band for SAS.

5 Focus Area D: Issues Related to Initial Launch and Evolution of SAS and Band Planning

D.1. SAS deployment issues

A spectrum management system based on a SAS can be deployed gradually, utilizing the initial operating experiences and introducing more sophisticated features after the operation of the basic functions has been sufficiently verified. The sequence and the capabilities to be introduced in each phase would depend on the range of functions needed in the full-fledged deployment (e.g. degree of dynamism, scheme for using auctions), as well as on the policy issued by the Administration.

It may be beneficial to arrange a pilot first, before the launch with limited number of users and technologies, with limited degree of dynamism, using a rather simple policy as a basis of the operation. The results of the pilot should be analyzed and utilized in the initial full scale deployment.

In our view the functions at launch could cover:

- Basic spectrum offer, request and assignment mechanisms implemented.
- If multiple SASs in use, differentiate their responsibilities to a degree that full real-time synchronization is not needed
- Protection of Incumbents and PA users either based on static or semi-static protection contours or receiver locations.
- PA use with 1 year-long PAL's, no renewal mechanisms.
- FCC to issue the PAL's for the PA users.
- Predefined spectrum use fees
- GAA use based on license by rule, to be deployed in the manner that TVWS is deployed today, similar devices, use static "coverage contours" for GAA,
- static, pre-defined policy defined by the Commission

The SAS's capabilities could evolve over time towards more dynamic system that:

- assigns spectrum based both on long term and short term (on-demand) spectrum requirements of the users
- assigns spectrum and defines the allowed operational parameters based on the actual technical characteristics of the deployed technologies, taking into account the transmit and receive characteristics, actual locations, deployments and coverage areas,
- employs measurements done by the users about the radio conditions over their coverage area to create a Radio Quality Map, utilizes the results in interference avoidance and assignment optimization and takes active measures to minimize interference,

- automatic authorization methods are in use, in manner defined by the policy
- uses periodic long term and short term auction mechanisms, where applicable, for pricing the assigned spectrum, uses automatic billing mechanisms,
- does constant or frequent overall optimization of the spectrum use and allows dynamic spectrum offers and possible spectrum reclaim by the incumbents,
- uses classified federal spectrum filtered through "declassification" process,
- is connected on-line to the Commission through the administrative interface e.g. to have real time information about the applicable operational policy, issued authorizations for the PA users, use of adjacent bands and for reporting about assignments and interference

The backward compatibility should be taken into account when the SAS deployment roadmap is developed. It would be beneficial if the tuning range of the initially deployed devices would already cover the full band that will eventually be managed by the SAS. Furthermore, the devices to be used can be able to operate even if the capabilities of the SAS evolve, because many advanced functions can be taken into use simply by updating the operating software of within the AP's, eNB's or in the OA&M etc.

As the SAS can take into account the actual characteristics of the deployed equipment, those with better capabilities and characteristics may enjoy more relaxed operating parameters, while less evolved equipment may not be able to reach the same performance, but still be able to utilize the services of the SAS and get spectrum assignments. The performance issues may also be reflected in the spectrum pricing, so that good performance would allow lower pricing due to more efficient spectrum use capabilities.

D.2. Network deployment topologies and technologies

In our view the initial deployment topologies could be determined based on the initial applications and users. The available bandwidths, the temporal and geographical availability of the spectrum, maximum allowed transmit powers, which application require access to spectrum should all be taken into account.

We believe that as a starting point deployment of small cells should be allowed in densely populated areas, and that the high power rural case and backhaul should be allowed in sparsely populated areas. Especially in the rural case it would be beneficial if the maximum allowed power levels would not be limited to any small fixed value, but that the upper limit would be mainly set by the actual conditions related to avoidance of interference.

We believe that the SAS can and needs to be designed to be technology neutral, or to be able to support multiple technologies. One important design principle should be that the current and emerging wireless technologies could be used by the PA and GAA users in connection with the SAS with minimal hardware modifications, specific to the use of the SAS. This would allow the benefits of the economies of scale and help creating a larger market. It would be beneficial if new functionalities could be taken into use through software updates, not requiring specific hardware.

In distinguishing use and technology cases the following aspects should be considered:

- application characteristics, suitability for PA or GAA use, preferred PAL duration, feasibility to acquire authorization through auction
- deployment characteristics: network structure (e.g. hotspot or cellular), cell size (coverage) and geographical location. The coverage impacts the required transmit power
- employed radio technology
- service characteristics, including the traffic vs time, need to provide QoS

D.3. Partitioning of the band

The partitioning should be flexible to allow evolution of usages within the band. The SAS can support flexible partitioning. Backward compatibility of the devices if the band plan evolves is possible when their tuning range covers the full band.

D.4. Maximizing flexibility

The SAS is very flexible and can accommodate new spectrum uses and topologies, while supporting backward compatibility. The key to maximizing the flexibility is the sufficient tuning range of the equipment, already from the launch.

D.5. Testing, development and deployment

As explained in Section D1, we would support gradual deployment comprising of:

- targeted pilot to test the basic functionalities,
- initial deployment with basic functionalities,
- evolutionary steps as defined in a roadmap towards a full-fledged system deployment.

In our view it would be beneficial to involve several potential SAS manufacturers and/or SAS operators to work together starting from the definition of the requirements and test procedures up to verification of the fully functional system.

D.6. Outages and service breaks

It is important to ensure reliable operation of the SAS. The possibilities for outage or discontinued service must be minimized. For example the power supply should be implemented in a reliable manner. Use of multiple SASs in parallel would further increase the reliability of the management of the band.

Furthermore, a requirement for an automatic shut-down feature could be considered for the equipment operating in the shared spectrum band. It may be required that the equipment will automatically cease transmissions, if they cannot be in contact with the SAS within a required time. Such a mechanism is required for the use of TV White Spaces: if a master WSD fails to connect with the database in a required time it shall cease transmission and shall instruct the slaves attached to it to cease transmission.

6 References

[1] FCC DA 13-2213, GN Docket No. 12-354**,** *Call for papers on the proposed spectrum access system for the 3.5 GHz band*, Nov 18th, 2013

[2] FCC 13-144, GN Docket No. 12-354**,** *Commission seeks comment on licensing models and technical requirements in the 3550-3650 MHz band*, Nov 1st, 2013

[3] FCC 12-148, GN Docket No. 12-354, Amendment of the Commission's Rules with Regard to Commercial Operations in the 3550-3650 MHz Band, *Notice of Proposed Rulemaking, Dec 12th, 2012.*

[4] PCAST President's Council of Advisors on Science and Technology (PCAST) report: "Realizing the full potential of government-held spectrum to spur economic growth", http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast_spectrum_report_final_july_20_2012.pdf

[5] Preston Marshall, "Scalability, Density, and Decision Making in Cognitive Wireless Networks", Cambridge University Press, 2013.

[6] PAWS, Protocol to Access Spectrum Database, draft-ietf-paws-protocol-07

[7] "Trust in M2M Communication. The New Security Threats", Inhyok Cha et. al., IEEE Vehicular Technology Magazine, Sep. 2009.

[8] "Evolution of Trust Systems from PCs to Mobile Devices", Dolores Howry et. al, IEEE Vehicular Technology Magazine, Vol. 8, Issue 1, Mar. 2013, p 70-80.

InterDigital appreciates the Commission's consideration of its white paper and welcomes any questions concerning its technologies.

Respectfully submitted,

Mihaela Beluri

Member of Technical Staff, InterDigital Inc.

2 Huntington Quadrangle

Melville, NY 11747